

**CONTINUATION OF AN APPLICATION FOR A SEARCH WARRANT**

I, Heather Williamson, being duly sworn, state as follows:

**INTRODUCTION AND BACKGROUND**

1. I make this continuation as part of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), for information associated with an account that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. (“Apple”), an electronic communications service provided and/or remote computing service, headquartered at One Apple Park Way, Cupertino, California. The information to be searched is Apple ID “michaelrh1986@gmail.com” (the “**Subject Account**”), as described in the following paragraphs and in Attachment A. This search warrant will require Apple to disclose to the government copies of information (including the contents of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will then review that information to locate and seize the items described in Section II of Attachment B.

2. I am a Special Agent of the Drug Enforcement Administration (“DEA”) and have been so employed since January 2013. I am currently assigned to the Grand Rapids District Office. Previously, I was assigned to the Southwest Border Initiative Group-3 (“SWB-3”) and to the Los Angeles Strike Force for approximately six years. The Los Angeles Strike Force is an investigative group jointly led by the DEA and the FBI, and composed of several other federal, state, and local agencies

that is focused on the disruption of the Mexico-based Sinaloa Cartel. Prior to working as a DEA Special Agent, I completed 20 weeks of training at the DEA Academy in Quantico, Virginia, which included instruction in narcotics identification, detection, trafficking, and interdiction; money laundering techniques; asset identification, seizure, and forfeiture; and techniques used by narcotics traffickers to avoid detection by law enforcement officials. I have investigated drug trafficking organizations involved in violating various federal laws, including, but not limited to, unlawful importation of controlled substances; the distribution of controlled substances; manufacturing of controlled substances; and possession with intent to distribute controlled substances, including cocaine, methamphetamine, heroin, and other dangerous drugs; as well as money laundering. I have participated in investigations of unlawful drug trafficking and money laundering and, among other things, have conducted or participated in surveillance; execution of search warrants; debriefings of informants; reviewing of taped conversations and drug records; and have participated in investigations that include the interception of wire communications.

3. Through my training, education, and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed, the methods of payment for such drugs, the laundering of narcotics proceeds, and the dialect (lingo) and coded language used by narcotics traffickers. In connection with my duties, I investigate criminal violations of the federal and state controlled substance laws, including, but not limited to, conspiracy and attempt to possess with

intent to distribute and to distribute controlled substances, in violation of Title 21, United States Code, Section 846; possession with intent to distribute and distribution of controlled substances, in violation of Title 21, United States Code, Section 841(a)(1); use of communication facilities to facilitate drug trafficking offenses, in violation of Title 21, United States Code, Section 843(b); and offenses involving money laundering as well as conspiracy and attempt to do the same, in violation of Title 18, United States Code, Sections 1956 and 1957. Many of these investigations also involve firearms offenses, including violations of Title 18, United States Code, Sections 922 and 924.

4. The facts in this application come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This application is intended to show merely that there is sufficient probable cause for the requested warrant, and does not set forth all of my knowledge about this matter.

5. Based on my training and experience, the facts as set forth in this application, and my knowledge of this investigation, there is probable cause to believe that violations of 21 U.S.C. §§ 841(a)(1) and 846 have been committed, are being committed, and will be committed by MICHAEL THOMAS, a/k/a “Money,” and his associates, known and unknown. I further submit that there is probable cause to believe that the **Subject Account** is being used by THOMAS to facilitate his drug trafficking activities and that, finally, there is probable cause to search the information described in Attachment A for evidence of these crimes, as described more fully in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is a “district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. On August 9, 2023, the Court authorized a Search Warrant for this **Subject Account**, Case No. 1:23-mj-393-PJG, for information and evidence from September 26, 2022 to August 29, 2023. The probable cause from that search warrant is incorporated here.

8. Generally, the probable cause for the **Subject Account** can be summarized as follows:

- a. Since at least early 2023, the DEA, the Michigan State Police (“MSP”), and the MSP-sponsored Southwest Enforcement Team (“SWET”) have been investigating THOMAS<sup>1</sup> and other individuals that coordinate drug trafficking activities, and the movement of bulk cash throughout Western Michigan, to include Kent County and Ionia County.

---

<sup>1</sup> THOMAS’s criminal history includes state convictions for misdemeanor traffic violations, possession of marijuana, domestic violence, and felony convictions for del/mfg controlled substance- cocaine or heroin less than 50 grams, possession of a controlled substance- cocaine or heroin less than 25 grams, 3<sup>rd</sup> degree home invasion, possession of a firearm by a felon, 2<sup>nd</sup> offense notice habitual offender, resisting/obstructing/assault of a police officer and possession of methamphetamine/ecstasy.

- b. In January 2020, the United States Postal Inspection Service (“USPIS”) and the Metropolitan Enforcement Team (“MET”) investigated the attempted delivery of a package to 758 Prince Street SE, Grand Rapids, Michigan that contained one pound and 15.3 ounces of positively tested methamphetamine. (MET complaint # MET-04-20.) and further intercepted the delivery of a package to 750 Prince Street SE, Grand Rapids, Michigan that appeared to contain methamphetamine, but ultimately was found to be 1147.5 grams barium sulfate. Barium sulfate is known to your Affiant as being “imitation meth” and sold on the street as methamphetamine. Barium sulfate has the same look and consistency as crystal methamphetamine. During this time, investigators were conducting physical surveillance at 750 Prince Street and observed THOMAS approach the USPS mail carrier to inquire about the package. The mail carrier subsequently told THOMAS that he couldn’t deliver the package, at which time THOMAS offered the mail carrier money to deliver the package.
- c. On June 15, 2022, the Grand Rapids Police Department responded to 1011 Emerald Ave NE, Grand Rapids Michigan for a domestic assault complaint. After their arrival on scene, it appeared Michael and Kandice Thomas were the subjects who were involved in the domestic complaint. The above address is where both THOMAS and Kandice Thomas were living. While investigating the complaint, Kandice Thomas stated there was narcotics in the home that belonged to THOMAS and gave Grand Rapids Police and their narcotics investigating team permission to search the basement and kitchen area. After obtaining a search warrant for the home, they located scales,<sup>2</sup> methamphetamine, cocaine, multiple firearms, and U.S. currency in the amount of \$7,000. (GRPD Vice report # 22-032935.)
- d. MSP sponsored Upper Peninsula of Michigan (“UPSET”) had an ongoing narcotics investigation into THOMAS, as a supplier of methamphetamine to the Upper Peninsula of Michigan. In the fall of 2022, a subject was found to be in possession of approximately three (3) pounds of methamphetamine. The UPSET investigation has identified THOMAS as the source of supply for that methamphetamine.

---

<sup>2</sup> On November 15th, 2022, Officer Jake Bloom from Grand Rapids Vice Unit received the lab report pertaining to a fingerprint taken from the scale. The lab report indicated the fingerprint belonged to MICHAEL THOMAS.

- e. Between late 2022 and April 2023, investigators were provided information from multiple Michigan State Police Confidential Informants<sup>3</sup> stating that THOMAS, or “Money,” is involved in the distribution of large quantities of narcotics. Investigators were provided the telephone number (616) 240-6733, which was determined to be subscribed to THOMAS and associated to the **Subject Account**. CI# 3 and CI# 4 both purchased quantities of narcotics from THOMAS.
- f. On July 7, 2023, SWET investigators applied for and were granted a search warrant from the 61<sup>st</sup> District Court in Kent County for Meta/Facebook records belonging to an identified account of THOMAS. Upon receiving and examining the search warrant return records from Meta/Facebook, your affiant observed multiple conversations between THOMAS and other Meta/Facebook users over the Facebook Messenger platform. THOMAS was sending and receiving messages about drug transactions, prices of narcotics, and violence being brought to those who owed him money. For example, one message from THOMAS stated “25 a p,” which based on my training, experience and knowledge of this investigation, I believe that “2500 a p” and “25 a P” is used often by individuals dealing in narcotics meaning \$2,500 for a pound of crystal methamphetamine. This is a consistent price for methamphetamine in the greater Grand Rapids area.

**B. Seizure of 5 kilograms of Methamphetamine**

10. On August 30, 2023, during a traffic stop on westbound I-96 in Ionia County, investigators seized over 5 kilograms (and almost 11 pounds) of

---

<sup>3</sup> CI #1 has been deemed credible and reliable through conducting controlled purchases of narcotics and providing information resulting in the recovery of stolen goods.

CI # 2 has been deemed credible and reliable by providing substantial information regarding drug activity that has been independently verified from other law enforcement investigations and activities.

CI #3 has been deemed credible and reliable through controlled purchases of narcotics and information that was independently verified by SWET detectives.

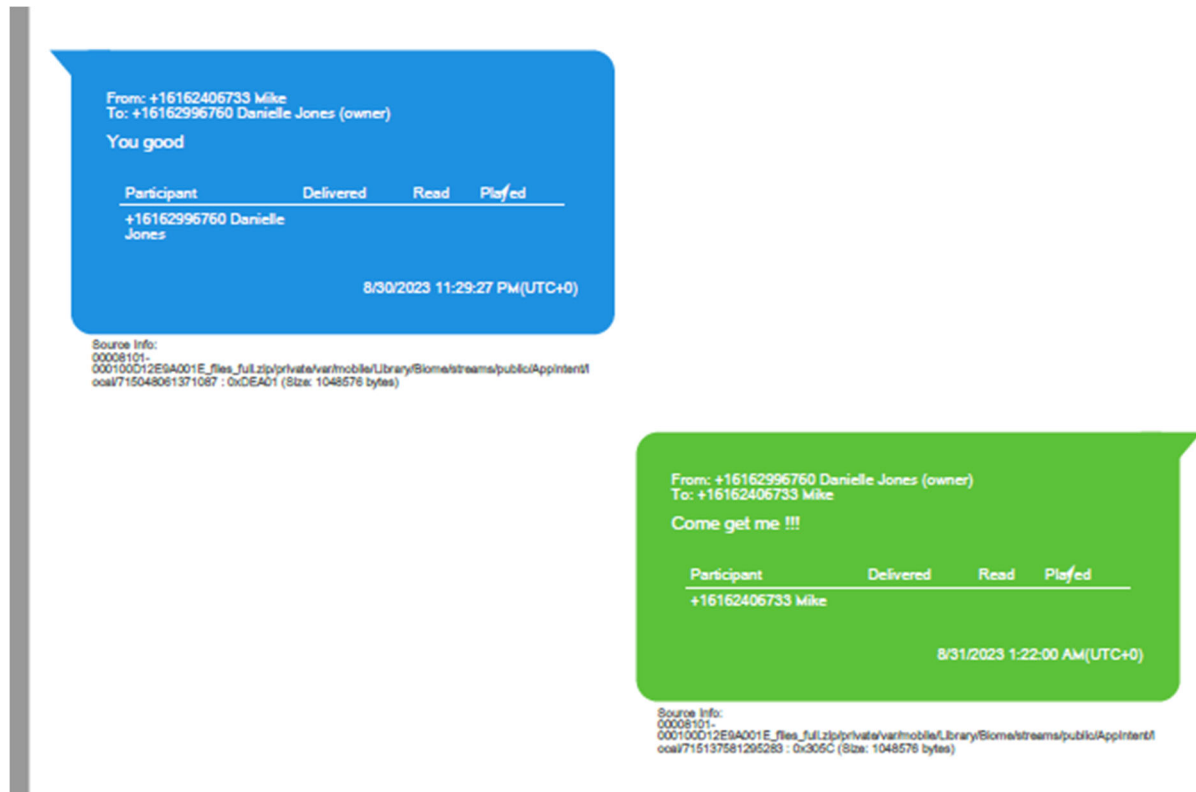
CI #4 has been deemed credible and reliable through controlled purchases of narcotics and information that has led to the arrest of larceny suspects.

methamphetamine from a car registered in THOMAS's name and driven and solely occupied by THOMAS's half-sister and co-defendant, DANIELLE LENA-MARY JONES, who was arrested that night and lodged at the Ionia County Jail.

11. During the traffic stop, JONES was using an iPhone and appeared to be texting on the iPhone. After her arrest, investigators seized the iPhone and searched it pursuant to a federal search warrant. *See* No. 1:23-mj-00404-RSK.

12. In JONES's iPhone, the phone number correlating to the **Subject Account** was saved under a contact named "Mike," as in MICHAEL OSBORN THOMAS.

13. Based on a review of text messages and call logs on JONES's iPhone, on August 30, 2023, beginning at approximately 7:39 a.m. and continuing through 9:22 p.m., there were approximately 13 Facetime contacts, 9 phone calls and a series of text messages between JONES and THOMAS, using the phone number associated to the **Subject Account**. Specifically, at approximately 9:22 pm., JONES sent a text message stating, "Come get me!!" along with a pin of her location. This correlates to the timing of the traffic stop discussed above, which happened around 9:00 p.m. (the timestamps in the screenshot below are UTC+0).



14. JONES also called THOMAS the following morning on August 31, 2023 from the Ionia County Jail.

15. On August 31, 2023, JONES was charged by federal criminal complaint in the Western District of Michigan with possession with intent to distribute a mixture and substance containing a detectable amount of methamphetamine, in violation of 21 U.S.C. §§ 841(a)(1), 841 (b)(1)(C). This Court issued a warrant for JONES's arrest. *See* Case No. 1:23-mj-00395. JONES had her initial appearance the same day, was appointed an attorney, and released on bond.

16. In September 2023, JONES participated in proffer interviews with investigators, identified THOMAS's phone number as (616) 240-6733, the phone



number associated to the **Subject Account**, and confirmed that she refers to THOMAS as “Mike.”

17. On August 30, 2023—the same day as the traffic stop and seizure of 5 kilograms of methamphetamine—investigators served the federal search warrant on Apple for records and information associated with the Apple ID account that belongs to THOMAS: “michaelrh1986@gmail.com.” Investigators seized data and messages between THOMAS and JONES’s iPhone from mid-2020 through August 29, 2023 that constitute evidence of THOMAS’s and JONES’s drug trafficking crimes.

18. For instance, THOMAS and JONES communicated about THOMAS storing drug proceeds at JONES’s residence, and at times, needing access to the money. On April 20, 2020, THOMAS messaged JONES: “Ik [I know] how much is there it better not be a dollar short but it can be a dolla more or even a few hundred more if you like.” JONES responded, “I don’t steal.” Ten days later, on April 30, 2020, THOMAS messaged JONES: “I need 2 bands [\$2,000]. Real quick.” JONES responded, “Ok.” THOMAS asked, “Do I gotta come get it, or can you bring it, I gotta take to kazoo [Kalamazoo]. Messages like this continued through 2023.

19. Messages between THOMAS and JONES also related directly to drug trafficking and facilitating drug deals. For example, between July 15 and July 20, 2021, THOMAS and JONES exchanged the following messages:

JONES: Can I do a half of one for now?

THOMAS: Yea

JONES: Alright bet.

When can I give you this money?

THOMAS: When ever you ready

JONES: I'm ready, how much?

THOMAS: It's 35 for whole if I stay up here 32 if I go to the d

JONES: I only want half

THOMAS: Ok

Based on my training and experience, I believe THOMAS and JONES were discussing quantities and prices of drugs, likely half-pound and pound quantities of methamphetamine. On October 8, 2022, THOMAS and JONES exchanged the following messages:

THOMAS: I need you to handle something for me

JONES: What's up

THOMAS: Ft [FaceTime] me asap

Call him when you get to the house

It's all a go waiting on you ft [FaceTime] me tho before you make a move

JONES: So imma have to wait at your house for an hour?

JONES: I'm about to head thay way now

What should it weight out

THOMAS: 448

Or 16 zips [ounces]

JONES: I knew that lbs

Same as [tree emoji, reference to marijuana]

THOMAS: Yea

Every person in play is stand up

Based on my training and experience and involvement in this investigation, I believe THOMAS had JONES go pick up a quantity of drugs, specifically 1 pound (16 ounces) of methamphetamine. I also know based on my training and experience that drug dealers regularly use FaceTime, an end-to-end encrypted video messaging service available on iPhones, to avoid law enforcement detection.

20. On September 27, 2023, investigators established physical and electronic surveillance on THOMAS in the vicinity of 1936 Stonebrook Circle, Grand Rapids, Michigan. Investigators subsequently coordinated the traffic stop of THOMAS utilizing marked Michigan State Police patrol cars, at which time THOMAS was taken into custody without incident on a federal arrest warrant for an indictment charging conspiracy to distribute controlled substances and other related offenses. Case No. 1:23-cr-117. Based on my training, experience and knowledge of this investigation, I believe the **Subject Account** will contain additional evidence of drug trafficking from the time of JONES arrest on August 30, 2023 to when investigators arrested THOMAS on September 27, 2023.

**C. Toll Analysis of Subject Account**

21. Investigators obtained toll records for numbers associated to THOMAS and JONES from August 1, 2023 to September 6, 2023. Utilizing the phone number associated to the **Subject Account**, THOMAS was in contact with JONES, using phone number (616) 299-6760, approximately 399 times and also using phone number

(616) 734-3202, approximately 136 times. Additionally, THOMAS was in contact with DORIAN TENNILLE,<sup>4</sup> using phone number (313) 690-8656, approximately 2 times on August 31, 2023.

22. Based on my training, experience, and knowledge of this investigation, I know that it is not uncommon for drug traffickers to utilize multiple cellphones. Specifically, drug traffickers frequently compartmentalize phone numbers for family members or certain members of their drug trafficking network that distribute various quantities and types of narcotics. Furthermore, I know it is common to utilize iCloud backup to transfer contacts, ongoing drug conversations and photographs among these various cellphones.

#### **BACKGROUND REGARDING APPLE<sup>5</sup>**

23. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

---

<sup>4</sup> (313) 690-8656 is subscribed to Dorian Armani Tennille, 34332 Marino St., Clinton Twp, MI 48035, with an associated email of [dorian.tennille@gmail.com](mailto:dorian.tennille@gmail.com).

On August 30, 2023, the Metro Narcotics Enforcement Team (“MNET”) observed JONES at 15285 Young Street, Detroit, MI prior to the traffic stop of 5 kilograms methamphetamine. MNET subsequently executed a State of Michigan search warrant on the location and located various documents in the name of Julius Williams, Jr and a security badge with a picture and name of TENNILLE.

<sup>5</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT2039943>; “iCloud,” available at <http://www.apple.com/icloud>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can

24. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud

---

I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

25. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services.

The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

26. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

27. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

28. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service,



including communications regarding a particular Apple device or service, and the repair history for a device.

29. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

30. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under

investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

31. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

32. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

33. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example,

information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

34. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

35. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

### **AUTHORIZATION REQUEST**

36. Based on the foregoing, I request that the Court issue the proposed search warrant.

37. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government

copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.